

A recursive construction of t -wise uniform permutations

Hilary Finucane* Ron Peled† Yariv Yaari‡

November 6, 2012

Abstract

We present a recursive construction of a $(2t + 1)$ -wise uniform set of permutations on $2n$ objects using a $(2t + 1) - (2n, n, \cdot)$ combinatorial design, a t -wise uniform set of permutations on n objects and a $(2t + 1)$ -wise uniform set of permutations on n objects. Using the complete design in this procedure gives a t -wise uniform set of permutations on n objects whose size is at most t^{2n} , the first non-trivial construction of an infinite family of t -wise uniform sets for $t \geq 4$. If a non-trivial design with suitable parameters is found, it will imply a corresponding improvement in the construction.

Keywords: t -wise permutation, combinatorial design, recursive construction.

1 Introduction

A t -wise uniform set of permutations is a subset of the symmetric group S_n which has the same statistics on any t -tuple as S_n . In other words:

Definition 1. A t -wise uniform set (of permutations on n objects) is a subset $T \subseteq S_n$ such that for any distinct $i_1, \dots, i_t \in [n]$ and any distinct $j_1, \dots, j_t \in [n]$, we have that the probability that $\sigma(i_m) = j_m$ for all $1 \leq m \leq t$ is the same whether σ is chosen uniformly from S_n or uniformly from T .

Equivalently, T is a t -wise uniform set if

$$\frac{1}{|T|} |\{\sigma \in T : \sigma(i_m) = j_m \text{ for } 1 \leq m \leq t\}| = \frac{1}{n(n-1) \cdots (n-t+1)} \quad (1)$$

for every distinct $i_1, \dots, i_t \in [n]$ and every distinct $j_1, \dots, j_t \in [n]$.

There are two *trivial* constructions of t -wise uniform sets: The symmetric group S_n is a t -wise uniform set for any $t \leq n$, and the alternating group A_n is a t -wise uniform set for

*Weizmann Institute of Science, Israel. Email: hilary.finucane@weizmann.ac.il. Supported by an ERC grant.

†Tel Aviv University, Israel. E-mail: peledron@post.tau.ac.il. Supported by an ISF grant and an IRG grant.

‡Weizmann Institute of Science, Israel.

$t \leq n - 1$ (and $n > 2$). In this paper we consider the problem of constructing non-trivial t -wise uniform sets.

The problem of finding explicit constructions for t -wise uniform sets was posed as an open problem by Kaplan, Naor, and Reingold in [5]. It was also shown there that *approximate* t -wise uniform sets of small size exist. Approximate t -wise uniform sets were further explored in [1], where Alon and Lovett showed that there exists a perfect t -wise uniform *distribution* over any approximate t -wise uniform set, a useful result for derandomization.

Non-trivial explicit constructions of (non-approximate) t -wise uniform sets for infinitely many n are known only for $t = 1, 2, 3$: the group of cyclic shifts $x \mapsto x + a$ modulo n is a 1-wise uniform set, the group of invertible affine transformations $x \mapsto ax + b$ over a finite field \mathbb{F} yields a 2-wise uniform set, and the group of Möbius transformations $x \mapsto (ax + b)/(cx + d)$ with $ad - bc = 1$ over the projective line $\mathbb{F} \cup \{\infty\}$ yields a 3-wise uniform set. Moreover, it is known (see for example [3, Theorem 5.2]) that for $n \geq 25$ and $t \geq 4$ there are no *subgroups* of S_n , other than A_n and S_n itself, that form a t -wise uniform set; such subgroups are called t -transitive subgroups of S_n . In contrast, it was shown recently [7] that for all $n \geq 1$ and $1 \leq t \leq n$, there exists a t -wise uniform set of permutations on n letters of size n^{ct} for some universal constant $c > 0$. For small t and large n , this result is close to the simple lower bound of $n(n-1) \cdots (n-t+1)$ which is implied by (1). It is important to emphasize, however, that the proof in [7] is purely existential and provides no hint as to the construction of such small t -wise uniform sets. Our work gives the first non-trivial explicit construction of an infinite family of t -wise uniform sets for $t \geq 4$.

A natural approach to constructing t -wise uniform sets is the divide-and-conquer method. To choose a permutation σ on $2n$ letters, it suffices to do the following.

Step 1. Choose the set $S \subseteq [2n]$ of n elements that will be mapped by σ to $1, \dots, n$.

Step 2. Choose two permutations τ_1 and τ_2 on n letters each to determine the behavior of σ on S and S^c .

If both steps are done independently and uniformly at random, then the resulting permutation σ is uniformly random. Moreover, if Step 1 is done uniformly at random and τ_1 and τ_2 are sampled independently (of each other and of S) and uniformly from two t -wise uniform sets, then the resulting family of permutations forms a t -wise uniform set. Indeed, in this case if $0 \leq m \leq t$, $1 \leq j_1, \dots, j_m \leq n$ and $n+1 \leq j_{m+1}, \dots, j_t \leq 2n$ are distinct indices and $1 \leq i_1, \dots, i_t \leq 2n$ are distinct indices, then

$$\begin{aligned} \Pr(\sigma(i_1) = j_1, \dots, \sigma(i_t) = j_t) &= \Pr(i_1, \dots, i_m \in S, i_{m+1}, \dots, i_t \notin S) \cdot \\ &\quad \cdot \Pr(\sigma(i_1) = j_1, \dots, \sigma(i_m) = j_m | i_1, \dots, i_m \in S, i_{m+1}, \dots, i_t \notin S) \cdot \\ &\quad \cdot \Pr(\sigma(i_{m+1}) = j_{m+1}, \dots, \sigma(i_t) = j_t | i_1, \dots, i_m \in S, i_{m+1}, \dots, i_t \notin S) \end{aligned}$$

and each term on the right hand side takes the same value whether S, τ_1 , and τ_2 are chosen independently and uniformly at random, or S is chosen uniformly at random and τ_1 and τ_2 are chosen independently and uniformly from t -wise uniform sets.

This observation gives us a naive approach to constructing t -wise uniform sets recursively. Letting $\text{Per}(n, t)$ denote the minimal size of a t -wise uniform set of permutations on

n elements, we obtain the recursion

$$\text{Per}(2n, t) \leq \binom{2n}{n} \text{Per}(n, t)^2. \quad (2)$$

We can use this recursion, together with the initial conditions $\text{Per}(n, t) = n!$ for $t \geq n$, to construct t -wise uniform sets; however, this recursion does not yield non-trivial constructions.

The first main contribution of this work is to propose an improved divide-and-conquer scheme for creating t -wise permutations. Specifically, adapting an idea proposed in [2], we observe that to construct a $(2t + 1)$ -wise uniform set of permutations on $2n$ elements, it suffices to use a $(2t + 1)$ -wise uniform set on n elements and a t -wise uniform set on n elements in Step 2 above, instead of two $(2t + 1)$ -wise uniform sets (see Figure 1). This yields the recursion:

$$\text{Per}(2n, 2t + 1) \leq \binom{2n}{n} \text{Per}(n, 2t + 1) \text{Per}(n, t), \quad (3)$$

where we define $\text{Per}(n, 2t + 1) = \text{Per}(n, n) = n!$ when $2t + 1 > n$. Unlike the naive recursion (2), this recursion yields a construction of a family of non-trivial t -wise uniform sets.

Theorem 1. $\text{Per}(n, t) \leq t^{2n}$ when n and t have the form $n = 2^m$ and $t = 2^\ell - 1$ for integers $m \geq 1$ and $\ell \geq 2$.

While t^{2n} is much smaller than the trivial upper bound $n!$, it is still much larger than the existence result of [7]. The second main contribution of this work is to suggest a potential extension that could lead to a smaller construction: Denoting by $\binom{[n]}{k}$ the set of subsets of $[n]$ of size exactly k , we suggest to replace the uniformly chosen set of n elements from Step 1 above with a set of n elements that is t -wise uniform, in the following sense.

Definition 2. A $(2n, t)$ -selection is a subset $\mathcal{S} \subseteq \binom{[2n]}{n}$ such that for all $I = \{i_1, \dots, i_t\} \subseteq [2n]$ and all $J \subseteq I$, the probability that $J \subseteq S$ and $I \setminus J \subseteq S^c$ is the same whether S is chosen uniformly from $\binom{[2n]}{n}$ or uniformly from \mathcal{S} .

A $(2n, t)$ -selection is equivalent to a $t - (2n, n, \cdot)$ combinatorial design (see Section 4). To obtain a t -wise uniform set, we can choose S uniformly from a $(2n, t)$ -selection in Step 1 above, rather than uniformly from $\binom{[2n]}{n}$. Letting $\text{Sel}(2n, t)$ denote the minimal size of a $(2n, t)$ -selection on $2n$ elements, this allows us to replace the naive recursion (2) with the following recursion:

$$\text{Per}(2n, t) \leq \text{Sel}(2n, t) \text{Per}(n, t)^2, \quad (4)$$

and the more powerful recursion (3) with:

$$\text{Per}(2n, 2t + 1) \leq \text{Sel}(2n, 2t + 1) \text{Per}(n, 2t + 1) \text{Per}(n, t). \quad (5)$$

These recursions imply that a non-trivial construction of a $(2n, t)$ -selection with the appropriate parameters will result in a non-trivial construction of a t -wise uniform set. For example, it is shown in [9] that a $(2n, t)$ selection (regarded as a $t - (2n, n, \cdot)$ design) must be of size at least $\binom{2n}{t/2}$ if t is even and of size at least $2\binom{2n-1}{(t-1)/2}$ if t is odd. If there were

an explicit construction of a $(2n, t)$ selection of size n^{ct} for some $c > 0$ (the existence of such a selection is proven in [7] but no explicit construction is known), then recursion (4) would lead to an explicit construction of a t -wise uniform set on n elements of size at most $(t+1)^{c'n}$ for some $c' > 0$ and recursion (5) would lead to a t -wise uniform set of size at most $2^{c_t(\log n)^{\log_2(t+1)}}$ for some $c_t > 0$ depending only on t . Thus our improved recursion allows us more efficiently to reduce the problem of finding t -wise uniform sets to the problem of finding $(2n, t)$ -selections. If a $(2n, t)$ -selection is allowed to be a multiset, then a reduction in the reverse direction holds as well: a $(2n, t)$ -selection \mathcal{S} can be obtained from a t -wise uniform set T by taking the family of sets of elements mapped to $1, \dots, n$ by the elements of T .

Unfortunately, we have been unable to come up with non-trivial constructions of $(2n, t)$ -selections with the appropriate parameters, or to find such constructions in the literature on combinatorial designs [4, 6]. Some more suggestions for extending our approach are described in Section 5.

2 The improved recursion

In this section we derive the recursion (5). Recursion (3) follows immediately by using the complete selection. For convenience, we will call a permutation chosen uniformly at random from a t -wise uniform set a *t -wise uniform permutation*.

Let A and B be t - and $(2t+1)$ -wise uniform sets on n elements, respectively, and let \mathcal{S} be a $(2n, 2t+1)$ -selection. For each $S \in \mathcal{S}$ let $f = f_S$ and $g = g_S$ denote bijections from S and S^c , respectively, to $[n]$. For each $\sigma \in A$, $\tau \in B$, and $S \in \mathcal{S}$ define a permutation $\mu_{S,\sigma,\tau}$ on $2n$ elements as follows:

$$\mu_{S,\sigma,\tau}(x) = \begin{cases} (\tau \circ \sigma)(f(x)) & x \in S \\ \tau(g(x)) + n & x \in S^c \end{cases} \quad (6)$$

The permutation $\mu_{S,\sigma,\tau}$ sends the elements of S to $\{1, \dots, n\}$ and the elements not in S to $\{n+1, \dots, 2n\}$. The behavior of $\mu_{S,\sigma,\tau}$ on S is determined by $\tau \circ \sigma$ and the behavior on S^c is determined by τ (see Figure 1).

Proposition 1. $\mathcal{M} = \{\mu_{S,\sigma,\tau} : S \in \mathcal{S}, \sigma \in A, \tau \in B\}$ is a $(2t+1)$ -wise uniform set.

Recursion (5) follows from the proposition since $|\mathcal{M}| \leq |\mathcal{S}||A||B|$. In the rest of this section we prove Proposition 1.

We start by introducing some notation. For a set of indices I , a function h and a set S , let $x_I = y_I$ denote $x_i = y_i$ for all $i \in I$, let $h(x_I) = y_I$ denote $h(x_i) = y_i$ for all $i \in I$, let $x_I \in S$ denote $x_i \in S$ for all $i \in I$, and let $x_I \notin S$ denote $x_i \notin S$ for all $i \in I$.

The key step in our proof of the proposition is the following lemma. It asserts that if σ and τ are t - and $(2t+1)$ -wise uniform permutations on $[n]$, respectively, independent of each other, then the pair of permutations $\tau \circ \sigma$ and τ , while neither uniform nor independent in general, behave exactly as uniform and independent when queried together on at most $2t+1$ inputs.

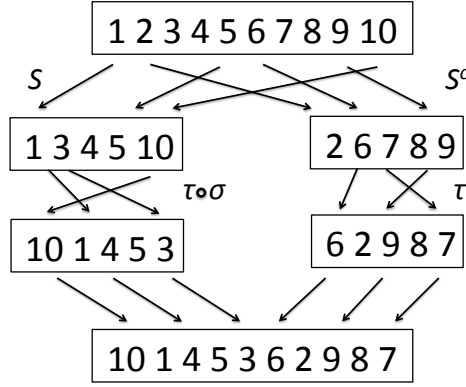


Figure 1: A $(2t+1)$ -wise permutation μ on $2n$ elements is constructed from a set S chosen from a $(2n, 2t+1)$ -selection, and permutations σ and τ drawn from t - and $(2t+1)$ -wise uniform sets of permutations on n elements, respectively. The behavior of μ on S is determined by $\tau \circ \sigma$, and the behavior of μ on S^c is determined by τ . Note that in this diagram, we are showing which number gets sent to which position; for example, $\mu(10) = 1$ and $\mu(1) = 2$.

Lemma 1. *Let σ and τ be t - and $(2t+1)$ -wise uniform permutations on $[n]$, respectively, independent of each other. For any $r, s \geq 0$ satisfying $r + s = 2t + 1$ and any distinct i_1, \dots, i_r , distinct j_1, \dots, j_r , distinct k_1, \dots, k_s , and distinct ℓ_1, \dots, ℓ_s in $[n]$, we have*

$$\Pr((\tau \circ \sigma)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]}) = \frac{(n-r)!(n-s)!}{n!^2}. \quad (7)$$

Proof. Fix r, s and sets of indices as in the lemma. Let

$$M = \{m_1 \in [r] : \text{there exists a } m_2 \in [s] \text{ such that } j_{m_1} = \ell_{m_2}\}.$$

For ease of notation, reorder the indices so that if $j_{m_1} = \ell_{m_2}$, then $m_1 = m_2$. Observe that on the event that $(\tau \circ \sigma)(i_{[r]}) = j_{[r]}$ and $\tau(k_{[s]}) = \ell_{[s]}$ we must also have that $\sigma(i_M) = k_M$ and $\sigma(i_b) \neq k_c$ for any $b \in [r] \setminus M$ and $c \in [s] \setminus M$. Let R denote the set of all permutations for which these two conditions hold; i.e.

$$R = \{\alpha \in S_n : \alpha(i_M) = k_M \text{ and } \alpha(i_b) \neq k_c \text{ for all } b \in [r] \setminus M \text{ and } c \in [s] \setminus M\}.$$

It follows that

$$\Pr((\tau \circ \sigma)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]}) = \Pr((\tau \circ \sigma)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]} \text{ and } \sigma \in R).$$

Breaking the event on the right-hand side into disjoint events based on the value σ takes,

and then using the independence of τ and σ , we have

$$\begin{aligned} \Pr((\tau \circ \sigma)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]}) &= \sum_{\alpha \in R} \Pr((\tau \circ \alpha)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]} \text{ and } \sigma = \alpha) \\ &= \sum_{\alpha \in R} \Pr((\tau \circ \alpha)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]}) \Pr(\sigma = \alpha). \end{aligned} \quad (8)$$

The definition of R shows that for any $\alpha \in R$ we have

$$\{(\tau \circ \alpha)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]}\} = \{(\tau \circ \alpha)(i_{[r] \setminus M}) = j_{[r] \setminus M}, \tau(k_{[s]}) = \ell_{[s]}\}.$$

Moreover, by the definitions of R and M , we know that the elements of $\alpha(i_{[r] \setminus M}) \cup k_{[s]}$ are all distinct and that the elements of $j_{[r] \setminus M} \cup \ell_{[s]}$ are distinct. Thus, recalling that $r + s = 2t + 1$ we can use the $(2t + 1)$ -wise uniformity of τ and equation (1) to write

$$\begin{aligned} \Pr((\tau \circ \alpha)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]}) &= \frac{1}{n \cdot (n - 1) \cdots (n - (r + s - |M|) + 1)} = \\ &= \frac{(n - r - s + |M|)!}{n!}. \end{aligned}$$

Hence we may continue (8) and obtain

$$\begin{aligned} \Pr((\tau \circ \sigma)(i_{[r]}) = j_{[r]}, \tau(k_{[s]}) = \ell_{[s]}) &= \\ &= \sum_{\alpha \in R} \frac{(n - r - s + |M|)!}{n!} \Pr(\sigma = \alpha) = \frac{(n - r - s + |M|)!}{n!} \Pr(\sigma \in R). \end{aligned} \quad (9)$$

Now let σ' be a permutation chosen uniformly at random from S_n . We claim that

$$\Pr(\sigma \in R) = \Pr(\sigma' \in R). \quad (10)$$

To see this, we consider separately the cases $r \leq t$ and $s \leq t$. One of these cases must hold since $r + s = 2t + 1$ by assumption. First, suppose $r \leq t$. We partition the event $\sigma \in R$ into disjoint events based on the values σ assigns to i_1, \dots, i_r , as follows.

$$\Pr(\sigma \in R) = \sum \Pr(\sigma(i_{[r]}) = x_{[r]}), \quad (11)$$

where the sum is taken over all sets of distinct $x_1, \dots, x_r \in [n]$ such that $x_M = k_M$ and $x_b \neq k_c$ for all $b \in [r] \setminus M$ and $c \in [s] \setminus M$. Now, since $r \leq t$ and σ is t -wise uniform, for each fixed x_1, \dots, x_r we have

$$\Pr(\sigma(i_{[r]}) = x_{[r]}) = \Pr(\sigma'(i_{[r]}) = x_{[r]}). \quad (12)$$

Combining (11) and (12) we obtain

$$\Pr(\sigma \in R) = \sum \Pr(\sigma(i_{[r]}) = x_{[r]}) = \sum \Pr(\sigma'(x_{[s]}) = k_{[s]}) = \Pr(\sigma' \in R),$$

where the sums are over the same choices of x_1, \dots, x_r as in (11).

The case $s \leq t$ proceeds similarly, by partitioning the event $\sigma \in R$ according to the inverse images of k_1, \dots, k_s through σ . We obtain

$$\Pr(\sigma \in R) = \sum \Pr(\sigma(x_{[s]}) = k_{[s]}) = \sum \Pr(\sigma'(x_{[s]}) = k_{[s]}) = \Pr(\sigma' \in R),$$

where the sum is taken over all sets of distinct $x_1, \dots, x_s \in [n]$ such that $x_M = i_M$ and $x_c \neq i_b$ for all $b \in [r] \setminus M$ and $c \in [s] \setminus M$. The second equality follows because $s \leq t$ and σ is t -wise uniform. Thus we have established (10) in all cases.

Finally, for the uniformly random permutation σ' it is straightforward to verify that

$$\Pr(\sigma' \in R) = \frac{(n-r)!(n-s)!}{(n-r-s+|M|)!n!}.$$

Thus the lemma follows from (10) and (9). \square

Proof of Proposition 1: To prove Proposition 1, we need to show that if μ is chosen uniformly at random from \mathcal{M} and $i_1, \dots, i_{2t+1} \in [2n]$ are distinct indices and $j_1, \dots, j_{2t+1} \in [2n]$ are distinct indices then

$$\Pr(\mu(i_{[2t+1]}) = j_{[2t+1]}) = \frac{(2n - (2t+1))!}{(2n)!}. \quad (13)$$

Fix two sets of distinct indices, $i_1, \dots, i_{2t+1} \in [2n]$ and $j_1, \dots, j_{2t+1} \in [2n]$. By reordering the indices, we may assume without loss of generality that $1 \leq j_1, \dots, j_m \leq n$ and $n+1 \leq j_{m+1}, \dots, j_{2t+1} \leq 2n$ for some $0 \leq m \leq 2t+1$. Observing that $(S_1, \sigma_1, \tau_1) \neq (S_2, \sigma_2, \tau_2)$ implies that $\mu_{S_1, \sigma_1, \tau_1} \neq \mu_{S_2, \sigma_2, \tau_2}$ we conclude that choosing an element μ uniformly at random from \mathcal{M} is equivalent to choosing elements S , σ , and τ uniformly at random and independently from \mathcal{S} , \mathcal{A} , and \mathcal{B} , respectively, and letting $\mu = \mu_{S, \sigma, \tau}$. Defining S , σ , τ and μ in this way, we have

$$\begin{aligned} \Pr(\mu(i_{[2t+1]}) = j_{[2t+1]}) &= \\ &= \Pr(i_{[m]} \in S, i_{[2t+1] \setminus [m]} \notin S, (\tau \circ \sigma \circ f)(i_{[m]}) = j_{[m]}, (\tau \circ g)(i_{[2t+1] \setminus [m]}) + n = j_{[2t+1] \setminus [m]}), \end{aligned}$$

where the equality $(\tau \circ g)(i_{[2t+1] \setminus [m]}) + n = j_{[2t+1] \setminus [m]}$ should be interpreted as $(\tau \circ g)(i_k) + n = j_k$ for all $k \in [2t+1] \setminus [m]$. Conditioning on S , we obtain

$$\begin{aligned} \Pr(\mu(i_{[2t+1]}) = j_{[2t+1]}) &= \\ &= \mathbf{E}(\mathbf{1}_{(i_{[m]} \in S, i_{[2t+1] \setminus [m]} \notin S)} \cdot \Pr((\tau \circ \sigma \circ f)(i_{[m]}) = j_{[m]}, (\tau \circ g)(i_{[2t+1] \setminus [m]}) + n = j_{[2t+1] \setminus [m]} \mid S)), \end{aligned} \quad (14)$$

where $\mathbf{1}_A$ denotes the indicator random variable of the event A . Now, recalling that τ and σ are independent of S , and that f and g depend only on S , we may apply Lemma 1 to conclude that for every S satisfying $i_{[m]} \in S$ and $i_{[2t+1] \setminus [m]} \notin S$ we have

$$\Pr((\tau \circ \sigma \circ f)(i_{[m]}) = j_{[m]}, (\tau \circ g)(i_{[2t+1] \setminus [m]}) + n = j_{[2t+1] \setminus [m]} \mid S) = \frac{(n-m)!(n-(2t+1-m))!}{n!^2}.$$

Substituting back into (14) yields

$$\Pr(\mu(i_{[2t+1]} = j_{[2t+1]}) = \frac{(n-m)!(n-(2t+1-m))!}{n!^2} \Pr(i_{[m]} \in S, i_{[2t+1] \setminus [m]} \notin S). \quad (15)$$

Since \mathcal{S} is a $(2n, 2t+1)$ -selection we have

$$\Pr(i_{[m]} \in S, i_{[2t+1] \setminus [m]} \notin S) = \frac{\binom{2n-(2t+1)}{n-m}}{\binom{2n}{n}}.$$

Substituting this into (15) yields

$$\Pr(\mu(i_{[2t+1]} = j_{[2t+1]}) = \frac{(2n-(2t+1))!}{(2n)!},$$

and the proposition follows. \square

Our construction is a modification of the method used in [2] for creating t -wise independent strings. In the context of that work, a (binary, unbiased) t -wise independent string is a random vector $X = (X_1, \dots, X_n) \in \{0, 1\}^n$ satisfying that $\Pr(X_i = 1) = 1/2$ for every i and that $(X_{i_1}, \dots, X_{i_t})$ are independent for every $1 \leq i_1 < \dots < i_t \leq n$. It was shown there that if X is a $(2t+1)$ -wise independent string and Y is a t -wise independent string (both of the same length) such that X and Y are independent then the string formed from the concatenation of X and $X+Y$ is $(2t+1)$ -wise independent. The proof there is similar to our own, but made easier by the fact that the group $\{0, 1\}^n$ is simpler than the group S_n and by the fact that no selection is necessary in the context of t -wise independent strings. It is of interest to understand the extent to which this method is applicable and find a common generalization of the above two scenarios.

3 The construction

In this section we use recursion (3) to construct an infinite family of non-trivial t -wise uniform sets, as stated in Theorem 1.

Proof of Theorem 1: We start by noting a few simple facts. First, we trivially have that $\text{Per}(n, t) = n! \leq t^{2n}$ when $t \geq n$. Second, we observe that the set of permutations $\{\sigma_b\}$, for $0 \leq b < n$, defined by $\sigma_b(i) = i + b \pmod{n}$ is a 1-wise uniform set of permutations on $\{0, \dots, n-1\}$. Thus, $\text{Per}(n, 1) \leq n$ for all n . (In fact, since $\text{Per}(n, t) \geq n(n-1) \cdots (n-t+1)$ by (1), this is an equality.)

Next, we establish the theorem for $t = 3$ (or $\ell = 2$). That is, we show that $\text{Per}(2^m, 3) \leq 3^{2^{m+1}}$ for all integer $m \geq 1$. The proof is by induction. For $m = 1$, we have $\text{Per}(2, 3) = 2 \leq 3^4$ as required. For $m > 1$, we have by equation (3), the above observations and the induction hypothesis that

$$\text{Per}(2^m, 3) \leq 2^{2^m} \text{Per}(2^{m-1}, 1) \text{Per}(2^{m-1}, 3) \leq 2^{2^m} 2^{m-1} 3^{2^m} = \frac{2^{2^m+m-1}}{3^{2^m}} 3^{2^{m+1}}.$$

It follows that $\text{Per}(2^m, 3) \leq 3^{2^{m+1}}$, as required, by using that $2^{(m-1)} \leq (3/2)^{2^m}$ for all $m \geq 2$ since $\log_2(3/2) \geq 1/2$ and $x \leq 2^x$ for $x \geq 1$.

Finally, we establish the theorem in general. We will prove by induction on m that for each $m \geq 1$, the claim holds for all $\ell \geq 2$. Again, the case $m = 1$ follows by our observation that $\text{Per}(n, t) = n! \leq t^{2^n}$ when $t \geq n$. Suppose that $m > 1$ and fix $\ell \geq 2$. We have already established the case $\ell = 2$ and the case $t \geq n$, so we may assume that $\ell \geq 3$ and satisfies $2^\ell - 1 < 2^m$. We also assume the induction hypothesis

$$\text{Per}(2^{m-1}, 2^{\ell'} - 1) \leq (2^{\ell'} - 1)^{2^m}$$

for all $\ell' \geq 2$. Thus, by (3),

$$\begin{aligned} \text{Per}(2^m, 2^\ell - 1) &\leq 2^{2^m} \text{Per}(2^{m-1}, 2^{\ell-1} - 1) \text{Per}(2^{m-1}, 2^\ell - 1) \leq \\ &\leq 2^{2^m} (2^{\ell-1} - 1)^{2^m} (2^\ell - 1)^{2^m} \leq (2^\ell - 1)^{2^{m+1}}, \end{aligned}$$

as required. □

4 The connection with t -designs

To obtain a smaller construction of a t -wise uniform set of permutations, it would suffice to construct a small $(2n, t)$ -selection that could be used in recursions (4) or (5). Selections are a special case of t -designs, defined as follows (see for example [4]):

Definition 3. A $t - (v, k, \lambda)$ design is a subset $\mathcal{S} \subseteq \binom{[v]}{k}$ satisfying that for every distinct $i_1, \dots, i_t \in [v]$ we have

$$|\{S \in \mathcal{S} : i_1, \dots, i_t \in S\}| = \lambda.$$

Thus, a $(2n, t)$ -selection is a $t - (2n, n, \lambda)$ design for some λ . The following simple lemma shows that the converse is also true (see for example [9, Proposition 1]):

Lemma 2. Let \mathcal{S} be a $t - (v, k, \lambda)$ design, $i_1, \dots, i_t \in [v]$, and $m \leq t$. Then the probability that $i_1, \dots, i_m \in S$ and $i_{m+1}, \dots, i_t \notin S$ is the same whether S is chosen uniformly from $\binom{[v]}{k}$ or uniformly from \mathcal{S} .

Thus, to improve the parameters of our construction using recursions (4) or (5), we need efficient $t - (2n, n, \lambda)$ designs for large n (and $t \geq 4$). However, we have not been able to find such designs in the literature.

5 Directions for future work

The parameters of our result could possibly be improved by considering a generalization of our construction that is based on an idea from [2]. The generalization is as follows: for any $k \geq 2$, a $(2t + 1)$ -wise uniform permutation on kn elements may be created from a uniformly random partition T of $[kn]$ into k groups of size n , and random permutations

$\tau, \sigma_1, \dots, \sigma_{k-1}$ where τ is a $(2t + 1)$ -wise uniform permutation on n elements and each σ_i is a t -wise uniform permutation on n elements, and $T, \tau, \sigma_1, \dots, \sigma_{k-1}$ are independent. The permutation is formed by partitioning the kn inputs to k groups according to T , applying τ to the first group and applying $\tau \circ \sigma_i$ to the $(i + 1)$ 'st group for $1 \leq i \leq k - 1$. The fact that the resulting permutation μ is $(2t + 1)$ -wise uniform follows easily from Lemma 1 and the simple observation that given any inputs i_1, \dots, i_{2t+1} to μ , and any choice of T , there can be at most one σ_i which determines the behavior of μ on more than t of these inputs. A significant advantage of this generalized construction is that although the number k can be arbitrarily large, still only one of the permutations used needs to be $(2t + 1)$ -wise uniform. Moreover, as in recursion (5), we may relax the condition that T be uniformly random to the condition that T be a $(2t + 1)$ -wise partition in an appropriate sense (though for $k \geq 3$ this notion is no longer connected with t -designs). We were unable to obtain any improvement in our parameters from this generalized construction, but we see it as a potential starting point for future improvements on our construction.

The construction in [2] was inspired by the $(u|u+v)$ method for combining error-correcting codes [8, p. 76]. Another promising direction for future research is to check whether other methods for combining codes can be adapted to yield constructions of t -wise uniform sets of permutations.

References

- [1] Noga Alon and Shachar Lovett. Almost k -wise vs. k -wise independent permutations, and uniformity for general group actions. *APPROX-RANDOM 2012*, pages 350–361, 2012.
- [2] Itai Benjamini, Ori Gurel-Gurevich, and Ron Peled. On k -wise independent distributions and boolean functions. *arXiv:1201.3261*, 2007.
- [3] P. J. Cameron. Permutation groups. In *Handbook of combinatorics, Vol. 1, 2*, pages 611–645. Elsevier, 1995.
- [4] Charles Colbourn and Jeffrey Dinitz. *Handbook of Combinatorial Designs*. Chapman & Hall/Taylor & Francis, 2007.
- [5] E. Kaplan, M. Naor, and O. Reingold. Derandomized constructions of k -wise (almost) independent permutations. In C. Chekuri, K. Jansen, J. D. P. Rolim, and L. Trevisan, editors, *Approximation, randomization and combinatorial optimization*, volume 3624 of *Lecture Notes in Computer Science*, pages 354–365. Springer, 2005.
- [6] Donald Kreher. Simple t -designs with large t : A survey. *Preprint*, see www.math.mtu.edu/~kreher/.
- [7] Greg Kuperberg, Shachar Lovett, and Ron Peled. Probabilistic existence of rigid combinatorial structures. *arXiv:1111.0492*, 2011.
- [8] Jessie MacWilliams and Neil Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library, 1977.

- [9] Dwijendra Kumar Ray-Chaudhuri and Richard Michael Wilson. On t -designs. *Osaka Journal of Mathematics*, 12:737–744, 1975.